

CLAIMS

What is claimed is:

- 1 1. A computerized method comprising:
 - 2 determining an active networked application;
 - 3 filtering a set of intrusion rules to create a subset of rules corresponding to the
 - 4 active networked application; and
 - 5 evaluating network traffic using the subset of rules.
- 1 2. The computerized method of claim 1 further comprising:
 - 2 detecting when the active networked application becomes inactive; and
 - 3 re-filtering the set of intrusion rules.
- 1 3. The computerized method of claim 2, wherein the detecting comprises:
 - 2 monitoring network connection terminations.
- 1 4. The computerized method of claim 2, wherein the detecting comprises:
 - 2 monitoring application terminations.
- 1 5. The computerized method of claim 1 further comprising:
 - 2 detecting when no networked application is active; and
 - 3 suspending the evaluating of network traffic until a networked application is active.
- 1 6. The computerized method of claim 1, wherein the subset of rules further
 - 2 corresponds to an operating system and further comprising:
 - 3 continuing the evaluating of network traffic if no networked application is active.

- 1 7. The computerized method of claim 1, wherein the determining comprises:
2 detecting when a network connection for an active application is initiated.
- 1 8. The computerized method of claim 1, wherein the filtering comprises:
2 marking an intrusion rule corresponding to the active networked application.
- 1 9. The computerized method of claim 1, wherein the filtering comprises:
2 extracting the subset of rules into an optimized set of rules.
- 1 10. The computerized method of claim 1, wherein the evaluating comprises:
2 analyzing network traffic on a port specified in the subset of rules.
- 1 11. The computerized method of claim 1, wherein the evaluating comprises:
2 analyzing network traffic for a protocol specified in the subset of rules.
- 1 12. The computerized method of claim 1, wherein the evaluating comprises:
2 discarding network traffic that satisfies at least one of the subset of rules; and
3 reporting an intrusion attempt.
- 1 13. The computerized method of claim 1, wherein the set of intrusion rules comprises
2 signatures of known attacks.
- 1 14. The computerized method of claim 1, wherein the set of intrusion rules comprises
2 heuristic rules.
- 1 15. A computer-readable medium having executable instructions to cause a computer
2 to perform a method comprising:
3 determining an active networked application;

4 filtering a set of intrusion rules to create a subset of rules corresponding to the
5 active networked application; and
6 evaluating network traffic using the subset of rules.

1 16. The computer-readable medium of claim 15, wherein the method further
2 comprises:
3 detecting when the active networked application becomes inactive; and
4 re-filtering the set of intrusion rules.

1 17. The computer-readable medium of claim 16, wherein the detecting comprises:
2 monitoring network connection terminations.

1 18. The computer-readable medium of claim 16, wherein the detecting comprises:
2 monitoring application terminations.

1 19. The computer-readable medium of claim 15, wherein the method further
2 comprises:
3 detecting when no networked application is active; and
4 suspending the evaluating of network traffic until a network application is active.

1 20. The computer-readable medium of claim 15, wherein the subset of rules further
2 corresponds to an operating system and the method further comprises:
3 continuing the evaluating of network traffic if no networked application is active.

1 21. The computer-readable medium of claim 15, wherein the determining comprises:
2 detecting when an active application initiates a network connection.

1 22. The computer-readable medium of claim 15, wherein the filtering comprises:
2 marking an intrusion rule corresponding to the active networked application.

1 23. The computer-readable medium of claim 15, wherein the filtering comprises:
2 extracting the subset of rules into an optimized set of rules.

1 24. The computer-readable medium of claim 15, wherein the evaluating comprises:
2 analyzing network traffic on a port specified in the subset of rules.

1 25. The computer-readable medium of claim 15, wherein the evaluating comprises:
2 analyzing network traffic for a protocol specified in the subset of rules.

1 26. The computer-readable medium of claim 15, wherein the evaluating comprises:
2 discarding network traffic that satisfies at least one of the subset of rules; and
3 reporting an intrusion attempt.

1 27. The computer-readable medium of claim 15, wherein the set of intrusion rules
2 comprises signatures of known attacks.

1 28. The computer-readable medium of claim 15, wherein the set of intrusion rules
2 comprises heuristic rules.

1 29. A system comprising:
2 a processor coupled to a memory through a bus; and
3 an intrusion prevention process executed from the memory by the processor to
4 cause the processor to determine an active networked application, to filter a set of intrusion
5 rules to create a subset of rules corresponding to the active networked application, and to
6 evaluate network traffic using the subset of rules.

1 30. The system of claim 29, wherein the intrusion prevention process further causes the
2 processor to detect when the active networked application becomes inactive, and to re-
3 filter the set of intrusion rules.

1 31. The system of claim 30, wherein the intrusion prevention process further causes the
2 processor to monitor network connection terminations in detecting when the active
3 networked application becomes inactive.

1 32. The system of claim 30, wherein the intrusion prevention process further causes the
2 processor to monitor application terminations in detecting when the active networked
3 application becomes inactive.

1 33. The system of claim 29, wherein the intrusion prevention process further causes the
2 processor to detect when no networked application is active, and to suspend evaluating
3 network traffic until a network application is active.

1 34. The system of claim 29, wherein the intrusion prevention process further causes the
2 processor to further filter the intrusion rules based on an operating system and to continue
3 evaluating network traffic if no networked application is active.

1 35. The system of claim 29, wherein the intrusion prevention process further causes the
2 processor to detect when an active application initiates a network connection in
3 determining an active networked application.

1 36. The system of claim 29, wherein the intrusion prevention process further causes the
2 processor to mark an intrusion rule corresponding to the active networked application in
3 filtering the set of intrusion rules.

1 37. The system of claim 29, wherein the intrusion prevention process further causes the
2 processor to extract the subset of rules into an optimized set of rules in filtering the set of
3 intrusion rules.

1 38. The system of claim 29, wherein the intrusion prevention process further causes the
2 processor to analyze network traffic on a port specified in the subset of rules in evaluating
3 the network traffic.

1 39. The system of claim 29, wherein the intrusion prevention process further causes the
2 processor to analyze network traffic for a protocol specified in the subset of rules in
3 evaluating the network traffic.

1 40. The system of claim 29, wherein the intrusion prevention process further causes the
2 processor to discard network traffic that satisfies at least one of the subset of rules, and to
3 report an intrusion attempt in evaluating the network traffic.

1 41. The system of claim 29, wherein the set of intrusion rules comprises signatures of
2 known attacks.

1 42. The system of claim 29, wherein the set of intrusion rules comprises heuristic rules.

1 43. An apparatus comprising:
2 means for determining when an active application becomes an active networked
3 application;
4 means for filtering coupled to the means for determining to create a subset of rules
5 corresponding to the active networked application from a set of intrusion rules; and
6 means for evaluating coupled to the means for filtering to evaluate network traffic
7 using the subset of rules.

1 44. The apparatus of claim 43, wherein the means for determining further detects when
2 the active networked application becomes inactive and the means for filtering further re-
3 filters the set of intrusion rules when the active networked application becomes inactive.

1 45. The apparatus of claim 43, wherein the means for determining further detects when
2 no networked application is active and the means for evaluating further suspends the
3 evaluation of network traffic until the means for determining determines a networked
4 application is active.

1 46. The apparatus of claim 43, wherein the means for filtering further filters the
2 intrusion rules corresponding to an operating system and the means for evaluating
3 continues the evaluation of network traffic when the means for determining determines no
4 networked application is active.

1 47. The apparatus of claim 43, wherein the means for evaluating comprises:
2 means for discarding network traffic that satisfies at least one of the subset of rules;
3 and
4 means for reporting an intrusion attempt.